

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-204701

(43) 公開日 平成8年(1996)8月9日

(51) IntCl.

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/00

9/10

9/12

H 0 4 L 9/ 00

Z

9466-5K

11/ 20

1 0 1 B

審査請求 未請求 請求項の数10 O L (全 19 頁) 最終頁に続く

(21) 出願番号 特願平7-10741

(22) 出願日 平成7年(1995)1月26日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 植田 広樹

東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内

(72) 発明者 宮口 庄司

東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内

(74) 代理人 弁理士 伊東 忠彦

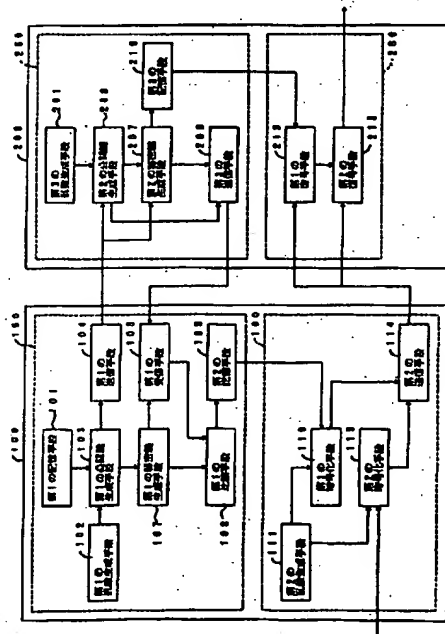
(54) 【発明の名称】 電子メール暗号通信システム及び暗号通信方法

(57) 【要約】

【目的】 本発明の目的は、第3者による意図的な通信データ監視による情報漏洩を不可能にし、送信側端末と受信側端末間における送信データの機密性を高めることが可能な電子メール暗号システム及び暗号化装置を提供することである。

【構成】 本発明は、受信端末200が共通鍵を生成するためのデータを送信し、受信したデータに基づいて共通鍵を生成し、共通鍵の部分鍵を送信端末100に送信する共通鍵生成処理手段150、250と、共通鍵生成処理手段150により生成された共通鍵を用いて暗号文を生成し、受信端末に送信し、受信端末が暗号文を共通鍵を用いて復号化するデータ転送処理手段160、260とを有する。

本発明の原理構成図



【特許請求の範囲】

【請求項 1】 暗号化された文書を送信する送信端末と、該送信端末より受信した文書を復号化する受信端末より構成される暗号通信システムにおいて、前記受信端末と前記送信端末との間で共有する共通鍵を生成するためのデータを前記送信端末に送信し、受信したデータに基づいて共通鍵を生成し、生成された該共通鍵の部分鍵を前記送信端末に送信し、前記送信端末側で該部分鍵に基づいて共通鍵を生成する共通鍵生成処理手段と、

前記共通鍵生成処理手段により生成された前記共通鍵を用いて、暗号文を生成し、前記受信端末に送信し、前記受信端末が該暗号文を前記共通鍵を用いて復号化するデータ転送処理手段とを有することを特徴とする電子メール暗号通信システム。

【請求項 2】 前記共通鍵生成処理手段において、前記送信端末は、予め装置毎に定めた n ビットの素数 P_A 、該素数 P_A の原始根 g_A を保持する第 1 の記憶手段と、乱数 r_A を生成する第 1 の乱数生成手段と、前記第 1 の記憶手段より前記素数 P_A 、原始根 g_A を取り出し、さらに、前記乱数 r_A を用いて巾乗演算を行い、第 1 の公開鍵 y_A を生成する第 1 の公開鍵生成手段と、前記素数 P_A 、前記原始根 g_A を前記第 1 の公開鍵生成手段より生成された前記第 1 の公開鍵 y_A と共に他装置に送信する第 1 の送信手段と、前記他装置から、前記他装置で生成された共通鍵の一部である部分鍵 $I D_B$ 及び第 2 の公開鍵 y_B を受信する第 1 の受信手段と、前記第 1 の受信手段により受信した前記第 2 の公開鍵 y_B と前記第 1 の公開鍵生成手段で用いた前記素数 P_A 、前記原始根 g_A により巾乗演算を行い、第 1 の鍵 K_A を生成する第 1 の秘密鍵生成手段と、前記第 1 の鍵 K_A の一部分を部分鍵 $I D_A$ とし、該部分鍵 $I D_A$ と前記部分鍵 $I D_B$ を比較する第 1 の比較手段と、前記第 1 の比較手段による比較の結果、一致する場合には、前記第 1 の鍵 K_A のビット列のうち、前記部分鍵 $I D_A$ にした部分とは異なる一部分を共通鍵 K_{AB} として、該共通鍵 K_{AB} を記憶する第 2 の記憶手段とを有し、

前記受信端末は、乱数 r_B を生成する第 3 の乱数生成手段と、前記送信端末から送信された前記素数 P_A 、前記原始根 g_A 及び公開鍵 y_A 、及び前記乱数 r_B を用いて巾乗演算を行い、前記第 2 の公開鍵 y_B を生成する第 2 の公開鍵生成手段と、前記第 2 の公開鍵生成手段で生成された前記第 2 の公開鍵 y_B 、前記素数 P_A 、前記乱数 r_B により巾乗演算を行い、第 2 の鍵 K_B を生成する第 2 の秘密鍵生成手段

と、前記第 2 の秘密鍵生成手段により生成された第 2 の鍵 K_B のビット列の一部分を部分鍵 $I D_B$ とし、第 2 の鍵 K_B のビット列のうち、該部分鍵 $I D_B$ に使用した部分以外の一部分を共通鍵 K_{AB} として格納する第 3 の記憶手段と、前記第 2 の公開鍵 y_B 及び前記部分鍵 $I D_B$ を前記送信端末に送信する第 3 の送信手段とを有する請求項 1 記載の電子メール暗号通信システム。

10 【請求項 3】 前記送信端末は、乱数 R_A を生成する第 2 の乱数生成手段と、前記乱数 R_A で前記第 2 の記憶手段に格納されている前記 K_{AB} を暗号化し、第 1 の暗号文 $E(K_{AB}, R_A)$ を生成する第 1 の暗号化手段と、前記乱数 R_A で本文 M を暗号化し、第 2 の暗号文 $E(M, R_A)$ を生成する第 2 の暗号化手段と、前記第 1 及び第 2 の暗号化手段で生成された前記第 1 の暗号文 $E(R_A, K_{AB})$ 及び前記第 2 の暗号文 $E(M, R_A)$ を送信する第 2 の送信手段とを有し、前記受信端末は、前記送信端末から受信した前記第 1 の暗号文 $E(K_{AB}, R_A)$ を用いて、前記第 3 の記憶手段に格納されている前記共通鍵 K_{AB} を用いて復号し、復号鍵 R_A を取得する第 1 の復号手段と、前記復号鍵 R_A を用いて、前記第 2 の暗号文 $E(M, R_A)$ を復号化して本文 M を取得する第 2 の復号手段とを有する請求項 1 記載の暗号通信システム。

【請求項 4】 前記送信端末は、前記本文 M のビット長を所定のビット列に変換し、変換データ $M I C$ を送信する変換・送信手段を有し、前記受信端末は、前記変換データ $M I C$ を受信すると、前記第 2 の復号化手段により取得した本文 M のビット長を所定のビット列に変換し、変換データ $M I C'$ を生成する第 1 の変換手段と、前記第 1 の変換手段により取得した変換データ $M I C'$ と受信した前記変換データ $M I C$ とを比較し、一致するかを判断する第 2 の比較手段とを更に有する請求項 3 記載の電子メール暗号化システム。

40 【請求項 5】 前記送信端末は、前記本文 M のビット長を所定のビット列に変換し、変換データ $M I C$ を生成する第 2 の変換手段と、前記変換データ $M I C$ と前記第 2 の乱数生成手段で生成された前記乱数 R_A を暗号化し、第 3 の暗号文 $E(M I C, R_A)$ を生成する第 3 の暗号化手段と、前記第 3 の暗号文 $E(M I C, R_A)$ を送信する第 4 の送信手段とを有し、前記受信端末において、前記第 4 の送信手段により送信された前記第 3 の暗号文 $E(M I C, R_A)$ を、前記第 1 の復号手段により取得

した前記復号鍵 RA を用いて前記第3の暗号文 $E(MIC, RA)$ を復号し、データ MIC を取得する第3の復号手段と、

前記第3の復号手段により取得した前記 MIC と、前記第2の復号手段により取得された前記本文 M とを比較して一致するかを判断する第3の比較手段を更に有する請求項3記載の暗号化システム。

【請求項6】 暗号化された文書を送信端末から電子メールで受信端末に送信し、該受信端末が該送信端末より受信した文書を復号化する暗号通信方法において、最初に、共通鍵生成処理として、

前記送信端末が前記受信端末に対して、共通鍵を生成するためのデータを送信し、

前記受信端末が、前記データを用いて共通鍵を生成し、該共通鍵の部分鍵を前記送信端末に送信し、

前記送信端末は、受信した前記部分鍵と、前記送信端末で生成した鍵とを比較して一致していれば、前記部分鍵を前記送信端末及び前記受信端末間において共通に使用する正当な共通鍵として保持し、

次に、データ転送処理として、前記共通鍵生成手段において、正当な共通鍵であることが確認された後、

前記送信端末は、前記共通鍵を用いてデータを暗号化して、前記受信端末に送信し、

前記受信端末は、前記共通鍵を用いて暗号化されたデータを復号することを特徴とする暗号通信方法。

【請求項7】 前記共通鍵生成処理において、

前記送信端末は、予め、素数 P_A 、該素数 P_A の原始根 g_A を保持しておき、

前記送信端末は、乱数 r_A を生成し、前記素数 P_A 、前記原始根 g_A により公開鍵 y_A を生成して前記受信端末に送信し、

前記受信端末は、乱数 r_B を生成し、前記送信端末より送信された前記素数 P_A 、前記原始根 g_A により公開鍵 y_B と鍵 K_B を生成すると共に、該鍵 K_B のある特定部分の m ビットを共通鍵 K_{AB} として保持し、該鍵 K_B の前記 m ビット以外の n ビットを部分鍵 ID_B として、該公開鍵 y_B と共に前記送信端末に送信し、

前記送信端末は、前記受信端末より受信した前記公開鍵 y_B と予め保持されている前記素数 P_A 、前記原始根 g_A を用いて鍵 K_A を生成し、該鍵 K_A のある特定部分の n ビットを部分鍵 ID_A とし、該部分鍵 ID_A と前記鍵 ID_B が一致しているかを検査し、

一致している場合には、前記鍵 K_A と前記鍵 K_B が等しいと見做し、前記鍵 K_A のある特定部分の m ビットを共通鍵 K_{AB} として保持する請求項6記載の暗号通信方法。

【請求項8】 前記データ転送処理において、

前記送信端末は、乱数 RA を生成し、

前記乱数 RA で前記共通鍵 K_{AB} を暗号化し、暗号文 E

(RA, K_{AB}) を生成し、

前記乱数 RA で本文 M を暗号化し、暗号文 $E(M,$

$RA)$ を生成し、前記暗号文 $E(RA, K_{AB})$ と該暗号文 $E(M, RA)$ を前記受信端末に送信し、前記受信端末に送信し、

前記受信端末は、前記共通鍵 K_{AB} を用いて前記暗号文 $E(RA, K_{AB})$ を復号化して復号鍵 RA を取得し、該復号鍵 RA により前記暗号文 $E(M, RA)$ を復号し、本文 M を取得する請求項6記載の暗号通信方法。

【請求項9】 前記データ転送処理において、

前記送信端末は、

10 前記本文 M をある長さの s ビット列に変換し、変換されたデータをデータ MIC とし、該データ MIC を前記受信端末に送信し、

前記受信端末は、

前記データ MIC を受信し、前記復号化された前記本文 M をある長さの s ビット列に変換し、データ MIC' とし、

受信した前記データ MIC と前記データ MIC' を比較して一致するか否かを判定する請求項8記載の暗号通信方法。

20 【請求項10】 前記データ転送処理において、

前記送信端末は、

前記本文 M をある長さの s ビット列に変換し、変換されたデータをデータ MIC とし、前記乱数 RA 及び該データ MIC を暗号化し、暗号文 $E(MIC, RA)$ を前記受信端末に送信し、

前記受信端末は、

前記復号鍵 RA を取得し、前記本文 M を取得した後に、前記本文 M を s ビット列に変換し、変換データ MIC' を取得し、

30 受信した前記暗号文 $E(MIC, RA)$ を復号した復号文 MIC を取得し、

前記変換データ MIC' と前記復号文 MIC を比較し、一致するか否かを判定する請求項8記載の暗号通信方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、電子メール暗号通信システム及び暗号通信方法に係り、特に、暗号化したデータを電子メールにより通信相手先に送信し、受信した電子メールを復号化する電子メールシステム上で、暗号通信を行う電子メール暗号通信システム及び暗号通信方法に関する。

【0002】近年、ネットワークが全世界的に広がり、基本的なコマンドを使用して端末間でテキストデータを送受信するメールシステムが使用されている中で、送信データの内容の漏洩を防止することが可能な電子メール暗号通信システム及び暗号通信方法が望まれている。

【0003】

【従来の技術】図12は、従来の2端末間のデータ転送の例を示す。同図に示す例は、ある端末AからデータM

5

が電子メールにて送信され、受信する端末を端末Bとし、端末A、B間が通信回線で直結している例である。この例の場合には、通信回線で、両端末が直結されているため、データMの内容が漏洩することなしに、受信者である端末Bに送信される。

【0004】図13は、従来の端末群内におけるデータの例を示す。同図に示す例は、ある端末Aから直接通信可能な端末群より1つの端末Cを選択し、データMを電子メールにて送信する。次に、端末AからデータMを受信した端末Cは、端末Bと直接通信可能なら、データMが最終的な送信先端末Bへ登録するためには、幾つかの端末を中継して送られる。なお、中継端末の選択は、電子メールシステムにおける経路制御と呼ばれるアルゴリズムによって制御される。

【0005】

【発明が解決しようとする課題】しかしながら、上記従来のメールシステムを利用してデータを送受信する場合、以下のような問題がある。即ち、送信側端末と受信側端末との間に幾つかの中継端末が存在しており、送信されるデータは、その中継端末間をそのままの形態で通過するために、中継端末上で、第3者の意図的な操作によるデータ内容の漏洩が可能性として生じる。さらに、ネットワークを構成している中継回線を第3者が直接監視した場合でも、データ内容を知ることが可能である。このため、ネットワークが発達した現在において、メールシステムによる機密性の高い情報を含んだデータを受信するには危険が伴うという問題がある。

【0006】本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、中継端末上または、中継回線において、第3者による意図的な通信データ監視による情報漏洩を不可能にし、送信側端末と受信側端末間における送信データの機密性を高めることが可能な電子メール暗号通信システム及び暗号通信方法を提供することを目的とする。

【0007】

【課題を解決するための手段】図1は、本発明の原理構成図である。本発明は、暗号化された文書を送信する送信端末100と、送信端末100より受信した文書を復号化する受信端末200より構成される暗号通信システムにおいて、受信端末200と送信端末100間において共通する共通鍵を生成するためのデータを受信端末200に送信し、受信したデータに基づいて共通鍵を生成し、共通鍵の部分鍵を送信端末100に送信し、送信端末側で部分鍵に基づいて共通鍵を生成する共通鍵生成処理手段150、250と、共通鍵生成処理手段150により生成された共通鍵を用いて、暗号文を生成し、受信端末に送信し、受信端末が暗号文を共通鍵を用いて復号化するデータ転送処理手段160、260とを有する。

【0008】本発明において、共通鍵生成処理手段150は、送信端末100が、予め装置毎に定めたnビット

6

の素数 P_A 、素数 P_A の原始根 g_A を保持する第1の記憶手段101と、乱数 r_A を生成する第1の乱数生成手段102と、第1の記憶手段101より素数 P_A 、原始根 g_A を取り出し、さらに、乱数 r_A を用いて巾乗演算を行い、第1の公開鍵 y_A を生成する第1の公開鍵生成手段103と、素数 P_A 、原始根 g_A を第1の公開鍵生成手段103より生成された第1の公開鍵 y_A と共に他装置に送信する第1の送信手段104と、他装置200から、他装置の部分鍵 I_{D_B} 及び第2の公開鍵 y_B を受信する第1の受信手段106と、第1の受信手段106により受信した第2の公開鍵 y_B と第1の公開鍵生成手段103で用いた素数 P_A 、原始根 g_A による巾乗演算を行い、第1の鍵 K_A を生成する第1の秘密鍵生成手段107と、第1の鍵 K_A の一部分を部分鍵 I_{D_A} とし、部分鍵 I_{D_A} と部分鍵 I_{D_B} を比較する第1の比較手段108と、第1の比較手段108による比較の結果、一致する場合には、第1の鍵 K_A のビット列のうち、部分鍵 I_{D_A} にした部分とは異なる一部分を共通鍵 K_{AB} として、共通鍵 K_{AB} を記憶する第2の記憶手段109とを有し、共通鍵生成処理手段250は、受信端末200が、乱数 r_B を生成する第3の乱数生成手段201と、送信端末100から送信された素数 P_A 、原始根 g_A 及び公開鍵 y_A 、及び乱数 r_B により巾乗演算を行い、第2の公開鍵 y_B を生成する第2の公開鍵生成手段203と、第2の公開鍵生成手段203で生成された第2の公開鍵 y_B 、素数 P_A 、乱数 r_B により巾乗演算を行い、第2の鍵 K_B を生成する第2の秘密鍵生成手段207と、第2の秘密鍵生成手段207により生成された第2の鍵 K_B のビット列の一部分を部分鍵 I_{D_B} とし、第2の鍵 K_B のビット列のうち、部分鍵 I_{D_B} に使用した部分以外の一部分を共通鍵 K_{AB} として格納する第3の記憶手段209と、第2の公開鍵 y_B 及び部分鍵 I_{D_B} を送信端末100に送信する第3の送信手段209とを有する。

【0009】また、データ転送処理手段160は、送信端末100が、乱数 R_A を生成する第2の乱数生成手段111と、乱数 R_A で第2の記憶手段109に格納されている K_{AB} を暗号化し、第1の暗号文 $E(K_{AB}, R_A)$ を生成する第1の暗号化手段110と、乱数 R_A で本文 M を暗号化し、第2の暗号文 $E(M, R_A)$ を生成する第2の暗号化手段113と、第1及び第2の暗号化手段110、113で生成された第1の暗号文及び第2の暗号文を送信する第2の送信手段114とを有し、データ転送処理手段260は、受信端末200が、送信端末100から受信した第1の暗号文 $E(R_A, K_{AB})$ を第3の記憶手段210に格納されている K_{AB} を用いて復号し、復号鍵 R_A を取得する第1の復号手段213と、復号鍵 R_A を用いて、第2の暗号文 $E(M, R_A)$ を復号化して本文 M を取得する第2の復号手段214とを有する。

【0010】また、上記のデータ転送処理手段160、

260において、送信端末100は、本文Mのビット長を所定のビット列に変換し、変換データMICを送信する変換・送信手段を有し、受信端末200は、変換データMICを受信すると、第2の復号化手段213により取得した本文Mのビット長を所定のビット列に変換する変換データMIC'を取得する第1の変換手段と、変換手段により取得したMIC'と受信した変換データMICとを比較し、一致するかを判断する第2の比較手段とを更に有する。

【0011】また、上記のデータ転送処理手段160、260において、送信端末100は、本文Mのビット長を所定のビット列に変換し、変換データMICを生成する第2の変換手段と、変換データMICと第2の乱数生成手段111で生成された乱数RAを暗号化し、第3の暗号文E(MIC, RA)を生成する第3の暗号化手段と、第3の暗号文E(MIC, RA)を送信する第4の送信手段とを有し、受信端末200は、第4の送信手段により送信された第3の暗号文E(MIC, RA)を、第1の復号手段213により取得した復号鍵RAを用いて第3の暗号文E(MIC, RA)を復号し、MICを取得する第3の復号手段と、第3の復号手段により取得したMICと、第2の復号手段214により取得された本文Mを比較して一致するかを判断する第3の比較手段をさらに有する。

【0012】図2は、本発明の原理を説明するためのシーケンスチャートである。本発明は、暗号化された文書を送信端末から電子メールで受信端末に送信し、受信端末が送信端末より受信した文書を復号化する暗号通信方法において、最初に、共通鍵生成処理として、送信端末が受信端末に対して、共通鍵を生成するためのデータを送信し(ステップ1)、受信端末が、データを用いて、共通鍵を生成し(ステップ2)、共通鍵の部分鍵を送信端末に送信し(ステップ3)、送信端末は、受信した共通鍵の部分鍵と、送信端末で生成した鍵とを比較して一致していれば、送信端末及び受信端末間において共通に使用する正当な共通鍵として保持し(ステップ4)、次に、データ転送処理として、共通鍵生成手段において、正当な共通鍵であることが確認された後、送信端末は、共通鍵を用いてデータを暗号化して(ステップ5)、受信端末に送信し(ステップ6)、受信端末は、共通鍵を用いて暗号化されたデータを復号する(ステップ7)。

【0013】また、上記の共通鍵生成処理において、送信端末は、予め、素数PA、素数PAの原始根gAを保持しておき、送信端末は、乱数rAを生成し、素数PA、原始根gAにより公開鍵yBを生成して受信端末に送信し、受信端末は、乱数rBを生成し、送信端末より送信された素数P、原始根gにより公開鍵yBと鍵KBを生成すると共に、共通鍵KBのある特定部分のmビットを共通鍵KABとして保持し、鍵KBのmビット以外のnビットを部分鍵IDBとして、公開鍵yBと共に送

信端末に送信し、送信端末は、受信端末より受信した公開鍵yBと予め保持されている素数PA、原始根gAを用いて鍵KAを生成し、鍵KAのある特定部分のnビットを部分鍵IDBとし、鍵IDAと鍵IDBが一致しているかを検査し、一致している場合には、鍵KAと鍵KBが等しいと見做し、鍵KAのある特定部分のmビットを共通鍵KABとして保持する。

【0014】また、上記のデータ転送処理において、送信端末は、乱数RAを生成し、乱数RAで共通鍵KABを暗号化し、暗号文E(RA, KAB)を生成し、乱数RAで本文Mを暗号化し、暗号文E(M, RA)を生成し、暗号文E(RA, KAB)と暗号文E(M, RA)を受信端末に送信し、受信端末は、共通鍵KABを用いて暗号文E(RA, KAB)を復号化して復号鍵RAを取得し、復号鍵RAにより暗号文E(M, RA)を復号し、本文Mを取得する。

【0015】また、上記のデータ転送処理において、送信端末は、本文Mをある長さのsビット列に変換し、変換されたデータをデータMICとし、データMICを受信端末に送信し、受信端末は、データMICを受信し、復号化された本文Mをある長さのsビット列に変換し、変換されたデータMIC'を取得し、受信したデータMICとデータMIC'を比較して一致するか否かを判定する。

【0016】また、上記のデータ転送処理において、送信端末は、本文Mをある長さのsビット列に変換し、変換されたデータをMICとし、乱数RA及びデータMICを暗号化し、暗号文E(MIC, RA)を受信端末に送信し、受信端末は、復号鍵RAを取得し、本文Mを取得した後に、本文Mをsビット列に変換し、変換データMIC'を取得し、受信した暗号文E(MIC, RA)を復号した復号文MICを取得し、変換データMIC'と復号文MICを比較し、一致するか否かを判定する。

【0017】

【作用】本発明は、送信端末と受信端末間で共通に有する共通鍵を生成する際に、受信端末で生成した鍵の部分鍵を送信端末に送信し、受信端末はその部分鍵を用いて共通鍵を生成する。これにより、共通鍵を送信端末、受信端末の両端末で共有する際に、通信路をいくつかのデータが通過するが、通信路を監視する第3者は、送信端末が生成する乱数rAを知り得ない限り共通鍵KABを知ることにはできない。ここで、素数PA及び原始根gAは通信路を通過するので、第3者がこれらを知ることが可能であるが、この2つの値から乱数rAを知ることが不可能である。なぜなら、離散対数問題と呼ばれ、この問題を多項式時間で解く有効なアルゴリズムは知られていないため、安全であるといえる。

【0018】また、両端末で計算された鍵KA(=KB)の一部分IDA(=IDB)として比較検査するため、送信端末側は鍵の共有が正しく行われたか否かを

9

確認することができる。この鍵共有は、特に支障のない限り、両端末で一度行うだけでよい。

【0019】また、データ転送においては、一般に本文Mは、そのデータ長が乱数 R_A より長いことが考えられるため、まず、乱数 R_A でデータを暗号化し、その後、この乱数 R_A を共通鍵 K_{AB} で暗号化する。一般に乱数 R_A が本文Mよりデータ長が長いことから、特に複数の受信者へ同一のデータを発信する同報通信時には、処理工程及び処理時間が短縮される。

【0020】

【実施例】以下、図面と共に、本発明の実施例を詳細に説明する。図3は、本発明の第1の実施例の暗号化装置の構成を示し、図4は、本発明の第1の実施例の復号化装置の構成を示す。なお、図3、図4において、説明の明瞭化のため、暗号化装置と復号化装置を別個に記載しているが、本来1つの端末装置に両方の機能を具備するものである。

【0021】図3において、送信側端末である暗号化装置100（以下、端末A）は、第1の記憶部101、第1の乱数生成器102、第1の中乗計算器103、第1のデータ送信部104、第2の記憶部105、データ受信部106、第2の中乗演算器107、比較器108、第3の記憶部109からなる鍵生成部150と、第1のデータ暗号化部110、第2の乱数生成器111、第4の記憶部112、第2のデータ暗号化部113、及び第2のデータ送信部114よりなるデータ転送部160から構成される。

【0022】図4において、復号化装置200（以下端末B）は、乱数生成器201、第1のデータ受信部202、中乗計算器103、第1の記憶部204、データ送信部205、及び第2の記憶部206からなる鍵生成部250と、第2のデータ受信部212、第1のデータ復号化部213、第2のデータ復号化部214、及び第3の記憶部215よりなるデータ転送部260より構成される。

【0023】なお、上記の図3、図4において、説明の明瞭化のため、同種の構成要素（例えば、送信部）が1つの端末に含まれているが、本来は1つずつの構成でよい。上記の端末Aの第1の記憶部101は、予め、端末毎に定めた素数 P_A とその原始根 g_A を格納しておき、さらに、第3の記憶部105は、送信先端末（復号化装置）毎に異なる鍵を共有するため、それらの鍵を格納する。

【0024】また、送信端末100と受信端末200間の通信はメールシステムにより行われるものとする。図5は、本発明の第1の実施例の動作を示すシーケンスチャートである。以下、図3、図4に示す各構成要素について図5に沿って説明する。

【0025】ステップ501） 端末Aの第1の乱数生成器102は、512ビット長の乱数 r_A を生成して、

10

第1の中乗計算器103に入力する。また、乱数 r_A は、以降の処理で再度使用するため、第2の記憶部105に記憶しておく。

ステップ502） 第1の中乗計算器103は、第1の記憶部101から素数 P_A と原始根 g_A を取り出し、第1の乱数生成器102により入力された乱数 r_A を用いて、

【0026】

【数1】

$$y_A = g_A^{r_A} \bmod P_A$$

【0027】（但し、上記の式は、 P_A を法とした剰余計算）を計算し、端末Aの公開鍵 y_A を生成し、素数 P_A と原始根 g_A と共に、第1のデータ送信部104に転送する。

ステップ503） 第1のデータ送信部104は、第1の中乗計算器103より転送された素数 P_A と原始根 g_A と公開鍵 y_A を端末Bに送信する。

【0028】ステップ504） 端末Bの第1のデータ受信部202は、端末Aから上記のデータを受信すると、第1の乱数生成器201により512ビットの長さの乱数 r_B を生成する。

ステップ505） 端末Bは、受信したデータ P_A と原始根 g_A と公開鍵 y_A と乱数 r_B を第1の中乗計算器203に入力し、

【0029】

【数2】

$$y_B = g_A^{r_B} \bmod P_A$$

【0030】（但し、上記の式は、 P_A を法とした剰余計算）を計算し、端末Bの公開鍵 y_B を取得する。さらに、

【0031】

【数3】

$$K_B = y_A^{r_B} \bmod P_A = g_A^{r_A r_B} \bmod P_A$$

【0032】（但し、上記の式は、 P_A を法とした剰余計算）を計算し、鍵 K_B を求める。

ステップ506） 次に、鍵を正しく共有化しているかを参照するための識別子として、鍵 K_B を2進数表示した際の0桁目から63桁目までを ID_B とし、また、端末Aと端末Bとの共通鍵として、64桁目から127桁目までを K_{AB} として設定し、第2の記憶部206に記憶する。

【0033】ステップ507） 端末Bは、第1の記憶部204から宛先である端末Aのアドレスを参照し、端末Aに対して、鍵 y_B と識別子 ID_B をデータ送信部209を介して端末Aに送信する。

ステップ508） 端末Aのデータ受信部106は、端末Bから鍵 y_B と識別子 ID_B を受信すると、第2の記憶部105に格納されている乱数 r_A を取り出し、第2の

巾乗計算器107に入力して、

【0034】

【数4】

$$K_A \equiv y \cdot s^A \pmod{P_A} \equiv g \cdot x^A \pmod{P_A}$$

【0035】(但し、上記の式は、 P_A を法とした剰余計算)により鍵 K_A を求める。

ステップ509) 上記の巾乗演算により求められた鍵 K_A により、鍵を正しく共有化しているかの識別子として、図6に示すように、 K_A を2進数表記した場合の0桁目から63桁目(64ビット)を識別子 ID_A とし、
10 端末Bより受信した識別子 ID_B と識別子 ID_A を比較器108に入力して比較する。等しい場合は、端末Aと端末Bとで、 $K_A = K_B$ であることが確認できる。図6の例では、512ビットのビット列を有するデータのうち、64ビットのID識別用601を用いて端末Aと端末BとのIDを比較し、同一であれば、次の64ビットの共通鍵602を K_{AB} として記憶しておくものである。

【0036】ステップ510) 上記のステップ509で $K_A = K_B$ が確認できた場合には、64桁目から127桁目までを共通鍵 K_{AB} として、第3の記憶部109に格納する。なお、上記の処理は、どちらかの端末から明示的に鍵を変更することをしない限り、ステップ501～ステップ510の処理は、最初に1度だけ実行しておき、記憶部に格納しておけばよい。

【0037】次に、端末Aと端末B間のデータ転送について説明する。

ステップ511) 端末Aの第2の乱数生成器111は、乱数 R_A を生成し、第1のデータ暗号化部110及び第2のデータ暗号化部113に入力する。

ステップ512) 第2の記憶部206から共通鍵 K_{AB} を読み出して、第1のデータ暗号化部110に入力し、
20 乱数 R_A を用いて共通鍵 K_{AB} を暗号化し、暗号文 $E(R_A, K_{AB})$ を取得する。

【0038】ステップ513) 第2のデータ暗号化部113は、本文 M が入力され、乱数 R_A により暗号化し、暗号文 $E(M, R_A)$ を取得する。

ステップ514) 第1のデータ暗号化部110は、暗号文 $E(R_A, K_{AB})$ を、第2のデータ暗号化部113は、暗号文 $E(M, R_A)$ を第2のデータ送信部114に転送し、第2のデータ送信部114は、暗号文 $E(R_A, K_{AB})$ と暗号文 $E(M, R_A)$ を端末Bに転送する。
40

【0039】ステップ515) 端末Bの第2の受信部212は、端末Aから送信された暗号文 $E(R_A, K_{AB})$ と暗号文 $E(M, R_A)$ を受信し、暗号文 $E(R_A, K_{AB})$ を第1の復号化部213に入力し、第2の記憶部210より共通鍵 K_{AB} を取り出して第1の復号化部213に入力して、復号化し、復号鍵として R_A を取得する。

【0040】ステップ516) 次に、復号鍵 R_A を第

2の復号化部214に入力し、暗号文 $E(M, R_A)$ を復号し、元の本文 M を取得する。

次に、データ転送処理の他の例を以下に示す。図8は、本発明の第2の実施例のデータ転送部の構成を示す。同図において、図3と同一構成部分には、同一符号を付し、その説明を省略する。端末Aにおいて、本文 M を s ビット列に変換するためのデータ変換部116を第1の実施例の図3のデータ転送部160の構成に加えた構成である。また、端末Bにおいても同様に本文 M を s ビット列に変換するためのデータ変換部216と、
10 端末Aから受信したデータとデータ変換部216で変換されたデータを比較するための比較部217をデータ転送部260に加えた構成である。

【0041】図9は、本発明の第2の実施例のデータ転送動作を示すシーケンスチャートである。上記の第1の実施例の図7に示すシーケンスチャートと同様の動作については、同一のステップ番号を付す。

ステップ511) 端末Aの第2の乱数生成器111は、乱数 R_A を生成し、第1のデータ暗号化部110及び第2のデータ暗号化部113に入力する。
20

【0042】ステップ512) 第2の記憶部206から共通鍵 K_{AB} を読み出して、第1のデータ暗号化部110に入力し、乱数 R_A を用いて共通鍵 K_{AB} を暗号化し暗号文 $E(R_A, K_{AB})$ を取得する。

ステップ513) 第2のデータ暗号化部113は、本文 M が入力され、乱数 R_A により暗号化し、暗号文 $E(M, R_A)$ を取得する。

【0043】ステップ513-1) 次に、データ変換部116は、本文 M を s ビット列に変換し、変換されたデータをMICとする。変換されるビット列は任意に設定可能である。

ステップ514-1) 第1のデータ暗号化部110は、暗号文 $E(R_A, K_{AB})$ を、第2のデータ暗号化部113は、暗号文 $E(M, R_A)$ を第2のデータ送信部104に転送し、第2のデータ送信部114は、暗号文 $E(R_A, K_{AB})$ と暗号文 $E(M, R_A)$ を端末Bに転送する。さらに、データ変換部116で変換されたデータMICも合わせて送信する。

【0044】ステップ515) 端末Bの第2の受信部212は、端末Aから送信された暗号文 $E(R_A, K_{AB})$ と暗号文 $E(M, R_A)$ 及びデータMICを受信し、暗号文 $E(R_A, K_{AB})$ を第1の復号化部213に入力し、第2の記憶部210より共通鍵 K_{AB} を取り出して第1の復号化部213に入力して、復号化し、復号鍵として R_A を取得する。

【0045】ステップ516) 次に、復号鍵 R_A を第2の復号化部214に入力し、暗号文 $E(M, R_A)$ を復号し、元の本文 M を取得する。

ステップ516-1) データ変換部216は、ステップ516で復号された本文 M を任意のビット列 s ビット

13

に変換し、データMIC'とする。

【0046】ステップ516-2) データ変換部216の出力であるMIC'と、第2のデータ受信部212で受信したMICを比較部217に入力し、MIC'とMICを比較し、一致しているか否かを判定する。このような方法によっても受信したデータが正しいか否かの判断が可能である。

【0047】図10は、本発明の第3の実施例のデータ転送部の構成図である。同図において、図3と同一構成部分には、同一符号を付し、その説明を省略する。端末Aにおいて、本文Mをsビット列に変換するためのデータ変換部116と、第2の乱数生成器111で生成された乱数RAを用いて、データ変換部116で変換されたデータを暗号化する第3のデータ暗号化部117を第1の実施例の図3のデータ転送部160に加えた構成である。また、端末Bにおいては、第2のデータ受信部212で受信した暗号化文のうち、上記の第2のデータ暗号化部117の出力である暗号文を復号する第3のデータ復号部218と、第2のデータ復号化部214で復号されたデータの任意のsビットの長さのデータに変換するデータ変換器220と、データ変換器220で変換されたデータと第3のデータ復号部218で復号されたデータを比較するための比較部219が図4のデータ転送部260に加えた構成である。

【0048】図11は、本発明の第3の実施例のデータ転送動作を示すシーケンスチャートである。同図において、上記の第1の実施例の図7と同様の動作については、同一のステップ番号を付す。

ステップ511) 端末Aの第2の乱数生成器111は、乱数RAを生成し、第1のデータ暗号化部110及び第2のデータ暗号化部113に入力する。

【0049】ステップ512) 第2の記憶部206から共通鍵KABを読み出して、第1のデータ暗号化部110に入力し、乱数RAを用いて暗号文E(RA, KAB)を取得する。

ステップ513) 第2のデータ暗号化部113は、本文Mが入力され、乱数RAにより暗号化し、暗号文E(M, RA)を取得する。

【0050】ステップ513-10) データ変換部116は、本文Mをsビット列に変換し、変換されたデータをMICとする。

ステップ513-11) 第3のデータ暗号化部117は、変換されたデータMICを乱数RAを用いて暗号化し、暗号文E(MIC, RA)を取得する。

【0051】ステップ514-10) 第2のデータ送信部114は、暗号文E(RA, KAB)と暗号文E(M, RA)及び暗号文E(MIC, RA)を端末Bに転送する。

【0052】ステップ515) 端末Bの第2の受信部212は、端末Aから送信された暗号文E(RA,

14

KAB)と暗号文E(M, RA)及び暗号文E(MIC, RA)を受信し、暗号文E(RA, KAB)を第1の復号化部213に入力し、第2の記憶部210より共通鍵KABを取り出して第1の復号化部213に入力して、復号化し、復号鍵RAを取得する。

【0053】ステップ516) 復号鍵RAで暗号文E(M, RA)を復号し、本文Mを取得する。

ステップ516-10) 復号された本文Mをデータ変換器220に入力し、sビット列のデータに変換し、変換データMIC'を得る。

【0054】ステップ516-20) 第3のデータ復号化部218は、復号鍵RAで暗号文E(MIC, RA)を復号し、データMICを取得する。

ステップ516-30) 変換データMIC'と復号されたデータMICを比較部219に入力し、比較し、同一であるか否かを判断する。

【0055】上記の第3の実施例も第2の実施例と同様に、受信側で受信したデータの正当性をチェックすることが可能となる。なお、本発明は、上記の実施例に限定されことなく、特許請求の範囲内で種々変更・応用が可能である。

【0056】

【発明の効果】上述のように本発明によれば、送信端末、受信端末共に鍵を共有し、データを暗号化して送信するものであり、鍵の共有化を行う段階では、通信路上に共通鍵KABが流れないこと、さらに、データ本文が暗号化されて通信路上を流れるために、通信路上を監視する第三者への情報の漏洩が発生しない。

【0057】また、鍵を共有する段階において、受信端末から共通鍵の一部を送信端末に送信し、送信端末において、比較検査することより、鍵の共有が正しくなされたか否かの検査が可能となるため、鍵の共有化がなされていないままデータを送信する無駄な操作が減少する。

【0058】また、データ本文を直接共通鍵で暗号化せず、乱数を用いて暗号化したのち、乱数を共通鍵で暗号化することは、データ本文の長さが長い場合、その暗号化に時間がかかるために、特に、同報通信を行う際に処理時間が短縮され、効率的である。

【図面の簡単な説明】

【図1】本発明の原理構成図である。

【図2】本発明の原理を説明するためのシーケンスチャートである。

【図3】本発明の第1の実施例の暗号化装置(端末A)の構成図である。

【図4】本発明の第1の実施例の復号化装置(端末B)の構成図である。

【図5】本発明の第1の実施例の鍵生成動作を示すシーケンスチャートである。

【図6】共通鍵検証に用いるビット列の例を示す図である。

15

【図7】本発明の第1の実施例のデータ転送動作を示すシーケンスチャートである。

【図8】本発明の第2の実施例のデータ転送部の構成図である。

【図9】本発明の第2の実施例のデータ転送動作を示すシーケンスチャートである。

【図10】本発明の第3の実施例のデータ転送部の構成図である。

【図11】本発明の第3の実施例のデータ転送動作を示すシーケンスチャートである。

【図12】従来の2端末間のデータ転送の例を示す図である。

【図13】従来の端末群内におけるデータの例を示す図である。

【符号の説明】

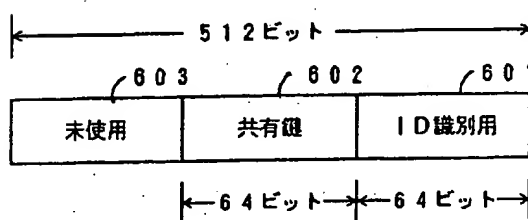
- 100 送信端末
- 101 第1の記憶手段、第1の記憶部
- 102 第1の乱数生成手段、第1の乱数生成器
- 103 第1の公開鍵生成手段、第1の巾乗計算器
- 104 第1の送信手段、第1のデータ送信部
- 105 第2の記憶部
- 106 第1の受信手段、データ受信部
- 107 第1の秘密鍵生成手段、第2の巾乗計算器
- 108 比較手段、比較器
- 109 第2の記憶手段、第3の記憶部
- 110 第1の暗号化手段、第1のデータ暗号化部
- 111 第2の乱数生成手段、第2の乱数生成器
- 113 第2の暗号化手段、第2のデータ暗号化部
- 114 第2の送信手段、第2のデータ送信部

16

- 116 データ変換部
- 117 第3のデータ暗号化部
- 150 鍵生成手段、鍵生成部
- 160 データ転送手段、データ転送部
- 200 受信端末
- 201 第3の乱数生成手段、乱数生成器
- 202 第1のデータ受信部
- 203 第2の公開鍵生成手段、巾乗演算器
- 204 第1の記憶部
- 205 データ送信部
- 206 第2の記憶部
- 207 第2の秘密鍵生成手段
- 208 第3の記憶手段
- 209 第3の送信手段
- 212 第2のデータ受信部
- 213 第1の復号手段、第1のデータ復号化部
- 214 第2の復号手段、第2のデータ復号化部
- 215 第3の記憶部
- 216 データ変換部
- 217 比較部
- 218 第3のデータ復号化部
- 219 比較部
- 220 データ変換器
- 250 鍵生成手段、鍵生成部
- 260 データ転送手段、データ転送部
- 601 ID識別用ビット
- 602 共通鍵用ビット
- 603 未使用ビット

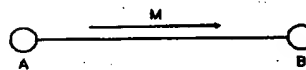
【図6】

共有鍵検証に用いるビット列の例



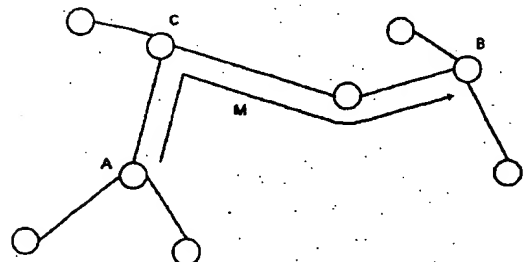
【図12】

従来の2端末間のデータ転送の例を示す図



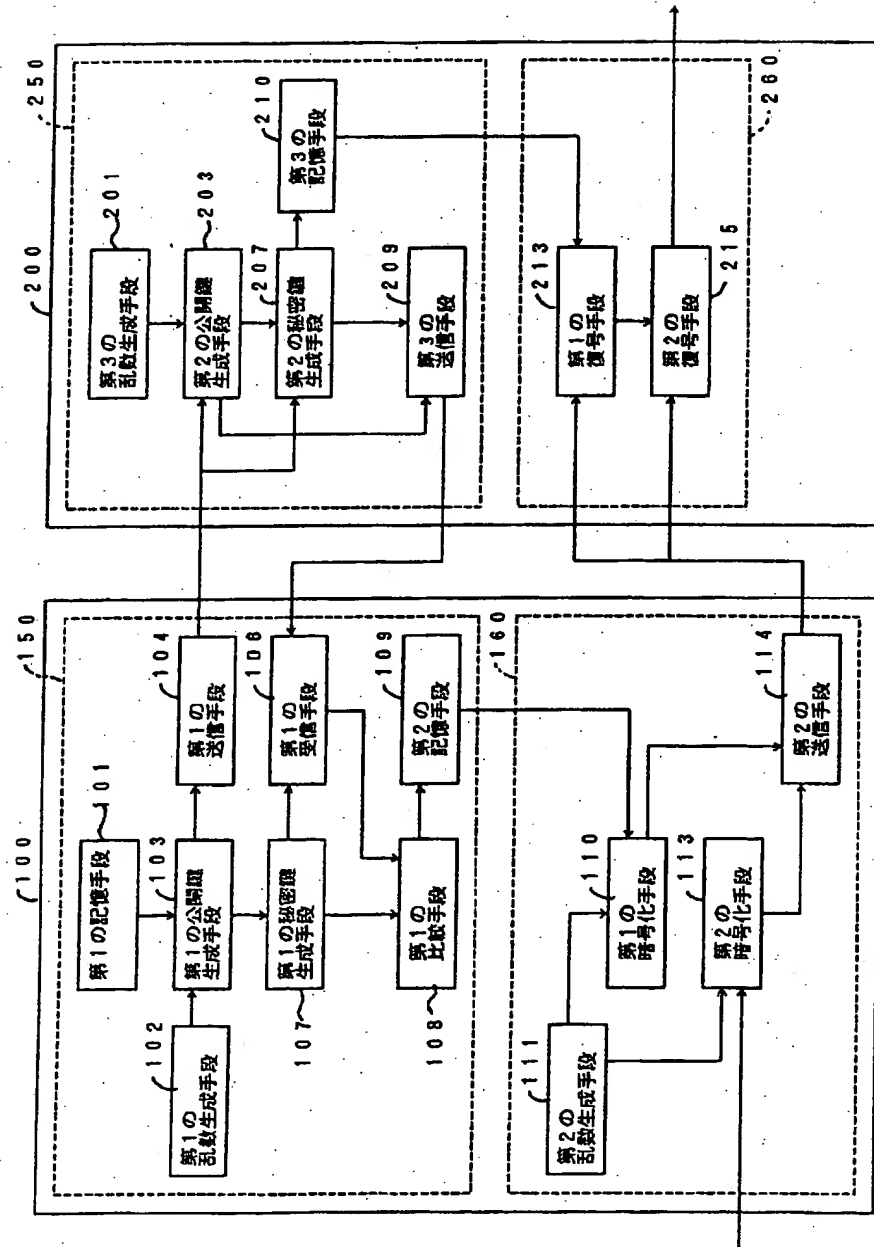
【図13】

従来の端末群内におけるデータの例を示す図



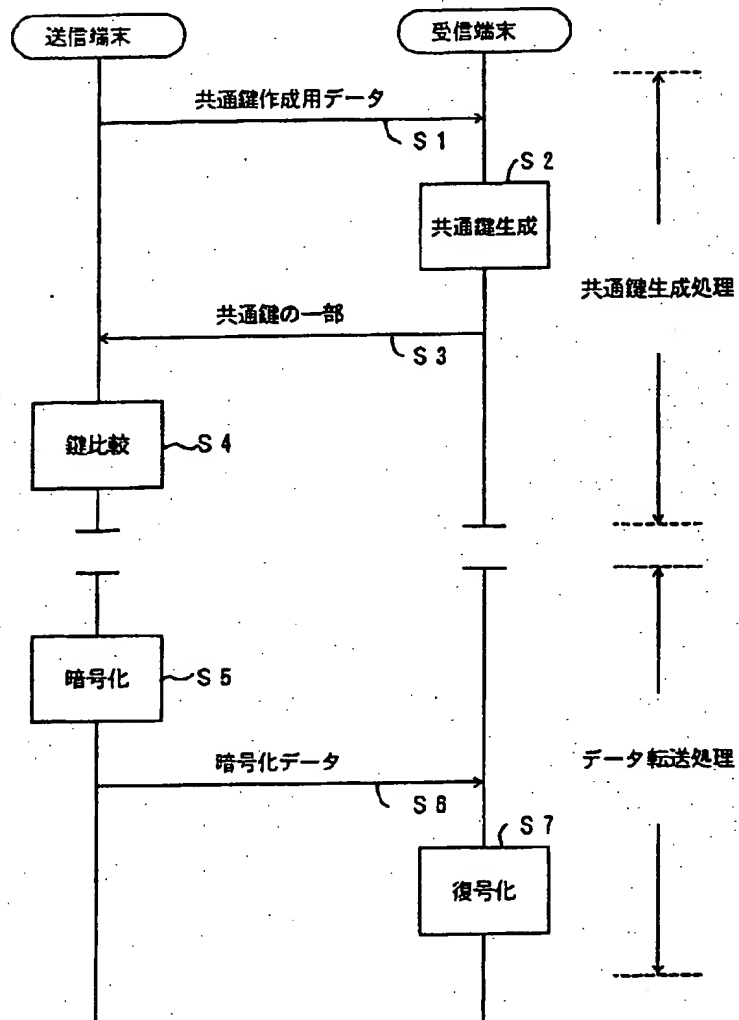
【図1】

本発明の原理構成図



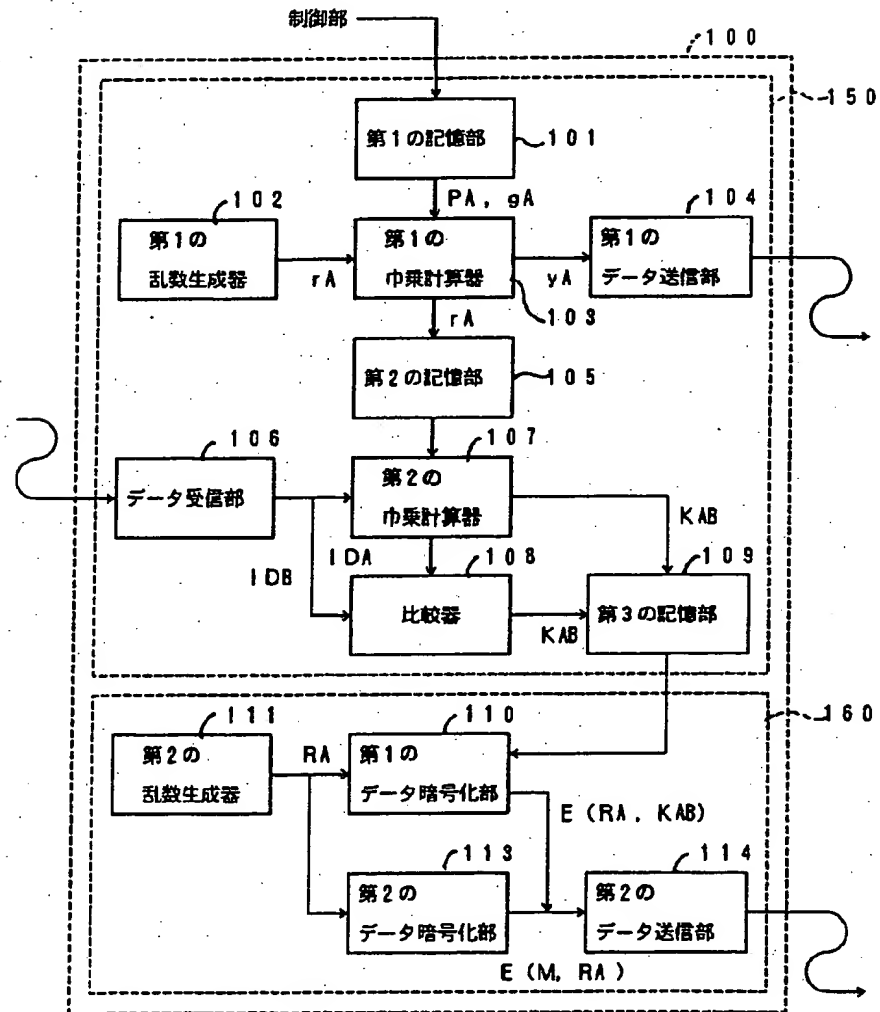
【図2】

本発明の原理を説明するためのシーケンスチャート



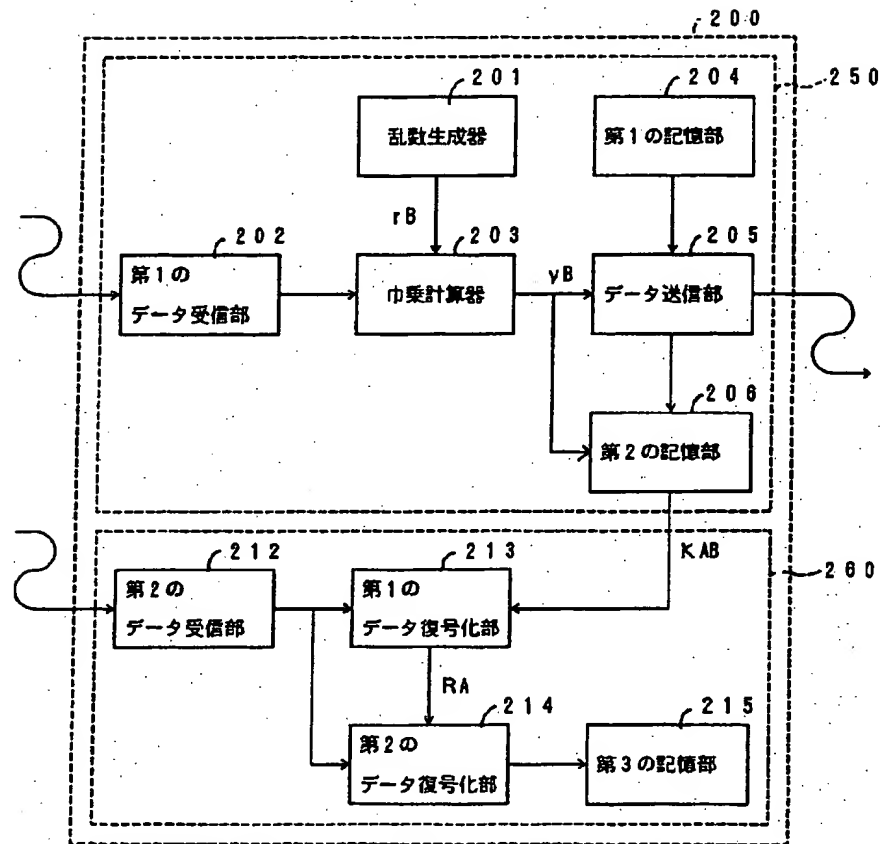
【図3】

本発明の第1の実施例の暗号化装置（端末A）の構成図



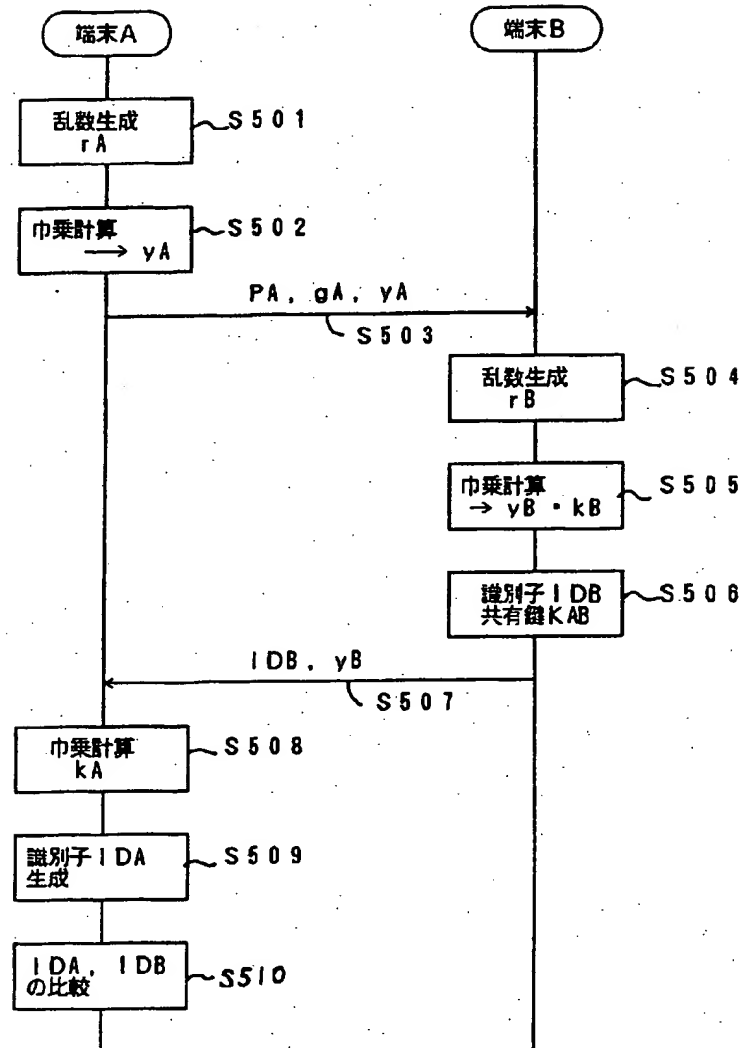
【図4】

本発明の第1の実施例の復号化装置（端末B）の構成図



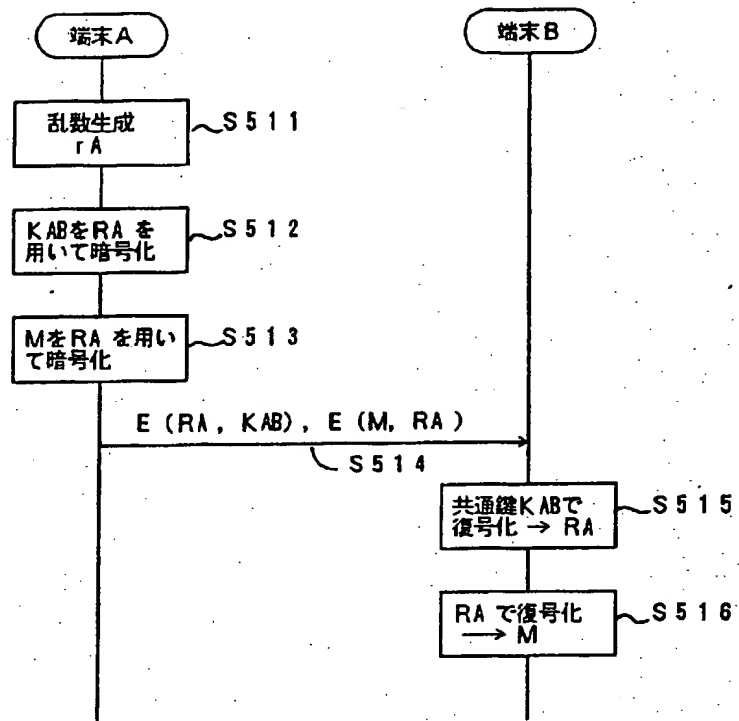
【図5】

本発明の第1の実施例の鍵生成動作を示すシーケンスチャート



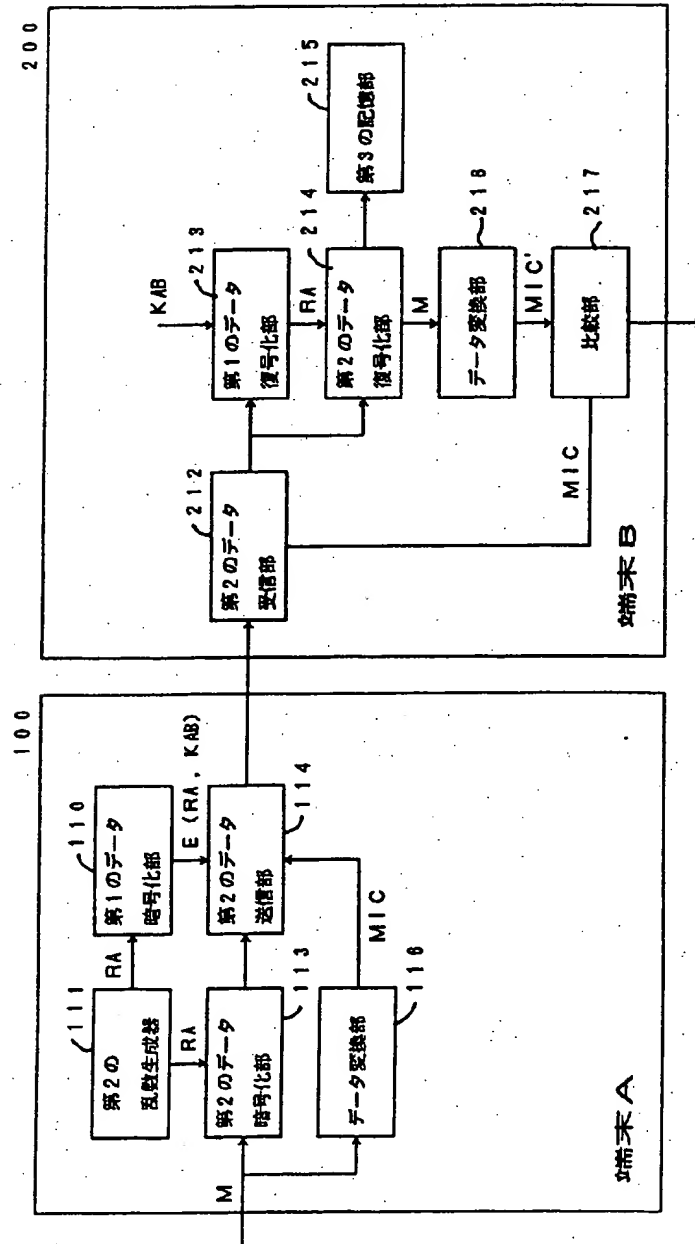
【図7】

本発明の第1の実施例のデータ転送動作を示すシーケンスチャート



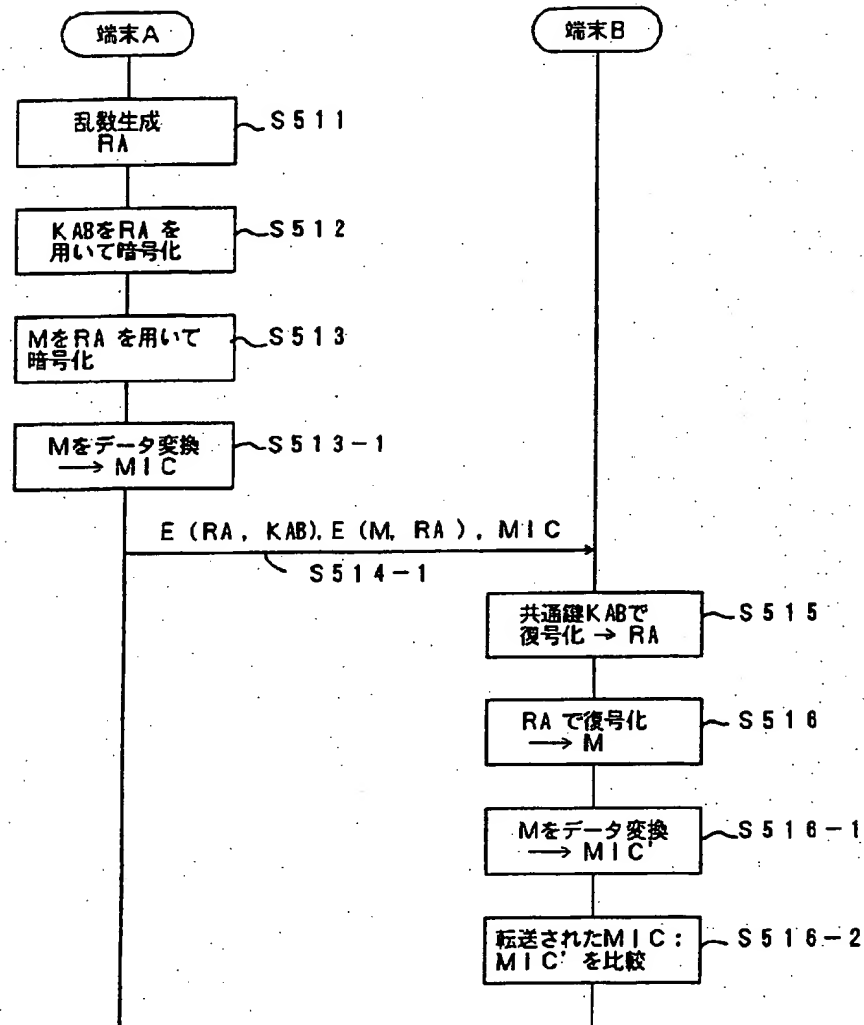
【図8】

本発明の第2の実施例のデータ転送部の構成図



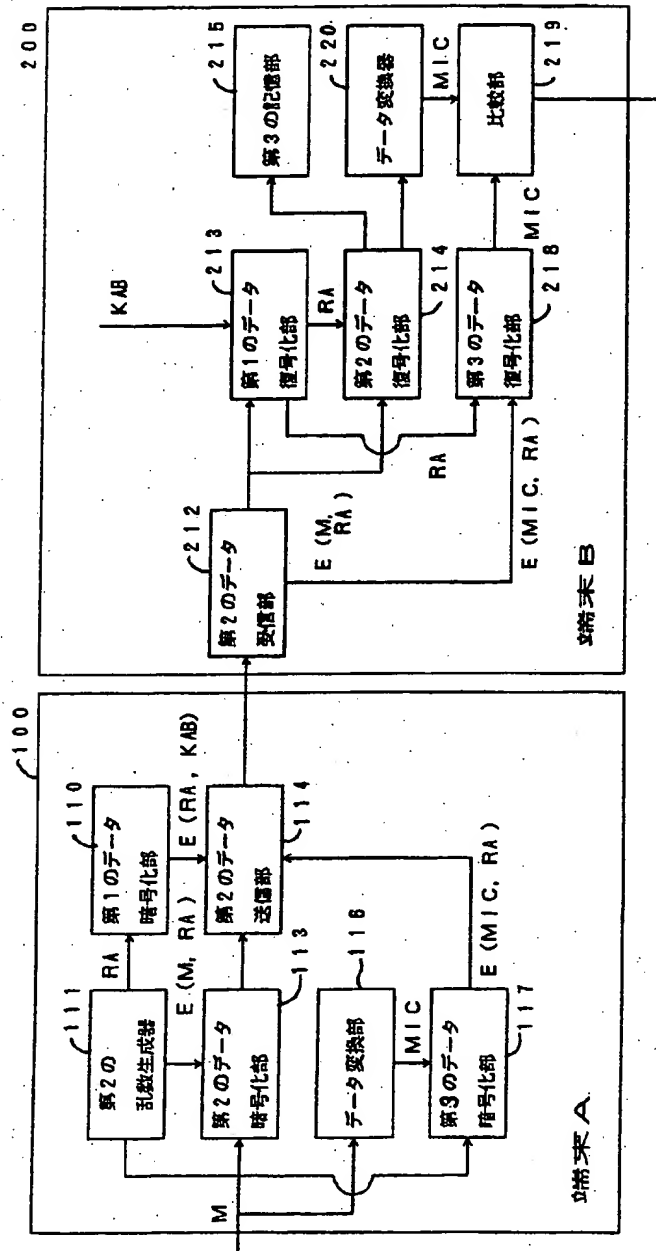
【図9】

本発明の第2の実施例のデータ転送動作を示すシーケンスチャート



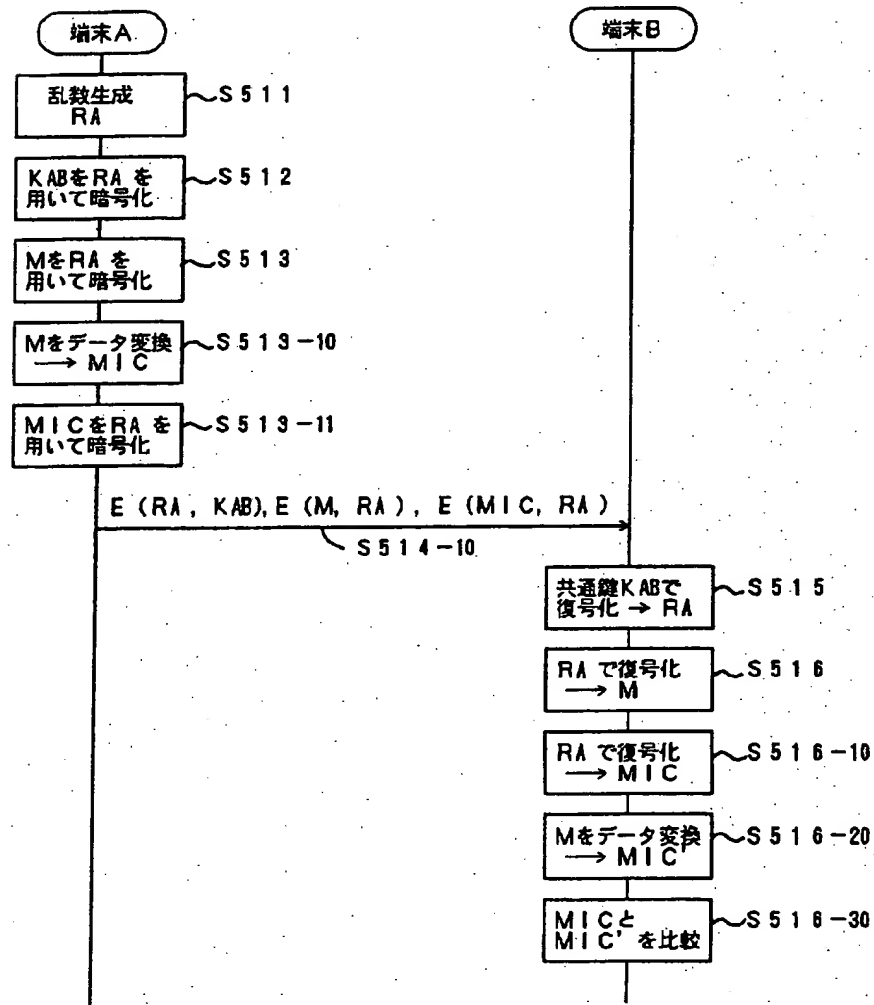
【図10】

本発明の第3の実施例のデータ転送部の構成図



【図11】

本発明の第3の実施例のデータ転送動作を示すシーケンスチャート



フロントページの続き

(51) Int. Cl.⁶

H04L 12/54

12/58

12/22

// G09C 1/00

識別記号

庁内整理番号

FI

技術表示箇所

7259-5J

9466-5K

H04L 11/26

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.